REMARKS

This Amendment is responsive to the Office Action mailed on October 17, 2007. Claims 7, 31, 32, and 36 are amended. Claims 1, 8, 9, and 41 are cancelled. Claims 2-7, 10-40, and 42 are pending.

The examiner has objected to the disclosure due to typographical errors on pages 3 and 7. The specification is amended herein to correct the typographical errors noted by the Examiner. Withdrawal of the objection to the specification is respectfully requested.

Claim 31 is objected to as lacking a period at the end of the claim. Claim 31 is amended herein to include a period. Withdrawal of this objection is respectfully requested.

Claims 1, 2, 4-14, and 17-42 are rejected under 35 U.S.C. § 102(e) as being anticipated by Alattar (US 7,020,304).

Claims 3, 15, and 16 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Alattar in view of Baker (US 6,912,010).

Discussion of Amended Claims

Claim 7 is amended to delete the word "all."

Claim 31 is amended to add a period at the end of the claim to overcome the Examiner's objection thereto.

Claim 32 is amended to delete "at least one of" so that the claim specifies that the received content is identified utilizing the fingerprint and the analyzing.

Claim 36 is amended to specify a watermark value rather than a watermark.

Discussion of Alattar

Claims 1, 2, 4-14, and 17-42 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Alattar. This rejection is respectfully traversed. An anticipation rejection requires that each and every element of the claimed invention as set forth in the claim be provided in the cited reference. See *Akamai Technologies Inc. v. Cable & Wireless Internet Services Inc.*, 68 USPQ2d 1186 (CA

FC 2003), and cases cited therein. As discussed in detail below, Alattar does not meet the requirements for an anticipation rejection.

Discussion of Independent Claim 2

Alattar discloses detecting a watermark with a payload that comprises different fields of information without the use of a fingerprint (Col. 10, lines 10-18, and Tables 1 and 2). Alattar at column 20, lines 1-57 describes an alternative system which combines the use of a watermark and a fingerprint, wherein the embedded watermark is used solely to provide a "*calibration signal, which is used to align the content before the fingerprint is computed.*" (Col. 20, lines 27-29). "*The calibration signal reduces the number of fingerprints that need to be maintained per content title in the fingerprint database.*" (Col. 20, lines 39-41). "*It then uses the calibration signal to align the data before computing the fingerprint.*"(Col. 20, lines 49-50) (Emphasis added).

The Alattar reference does not teach detecting any watermark value inserted in a given broadcast program and comparing the detected watermark value and derived fingerprint value from the given broadcast program with stored watermark and associated fingerprint values, as is claimed in Applicants' claim 2. In other words, in Applicants' claim 2, the watermark value that is extracted from the content, as well as the fingerprint value that is derived from the content is compared to the stored watermark and fingerprint values. Alattar does not derive a watermark value for use in conjunction with a fingerprint value; it rather uses the embedded watermark in solely for alignment purposes prior to computing the fingerprint. When both fingerprinting and watermarking techniques are utilized, Alatter does not compare a detected watermark value and a derived fingerprint value to stored watermark and fingerprint values.

Accordingly, Alattar does not disclose or remotely suggest the subject matter of Applicant's independent claim 2.

Discussion of Claim 5

Alattar does not disclose or remotely suggest, when a combination of watermarking and fingerprinting techniques are used, matching the detected watermark to stored watermark values,

and if a match is found, cross-checking the derived fingerprint value with the stored fingerprint value associated with said stored watermark, as set forth in Applicants' claim 5.

Discussion of Claim 6

US 2002/0126872 incorporated into Alattar and relied on by the Examiner does not disclose or remotely suggest sending the result of the cross-checking (of the derived fingerprint value with the stored fingerprint value associated with said stored watermark) to a registrant of the program. As best understood, US 2002/0126872, Par 39, lines 16-22, forwards the fingerprint, itself, to a private database to determine the version of content.

Discussion of Claim 7

US 2002/0126872 (or a combination thereof with Alattar) does not disclose or remotely suggest all the elements of claim 2, 5, and 7. Amended claim 7, which is dependent on claim 5, indicates that if the derived fingerprint is different from the stored fingerprint that is associated with the stored watermark, then the derived fingerprint is compared with the stored fingerprint values. US 2002/0126872, as best understood, describes using the fingerprint for identifying a content item, and using the watermark for providing "calibration data" or "additional information (owner ID, meta data, security information, etc."). In the case where the watermark carries calibration data (Alattar, Col. 20, lines 21-45), it is used to "realign (or retransform) the data before computing the signature" and not for comparing with the stored fingerprint values. In the case where the fingerprint is used to identify the content and the watermark carries additional information (US2002/0126872, Pars. 38 and 39), the central database determines from the digital watermark that the owner is Label X, and the content signature (i.e. the fingerprint value) is then forwarded to a different database to determine which version of the content is present.

Accordingly, Allatar, even taking into consideration US 2002/0126872, does not does not disclose or remotely suggest that, if the derived fingerprint is different from the stored fingerprint that is associated with the stored watermark, then to compare the derived fingerprint with the stored fingerprint values, as set forth in Applicants' claim 7.

Discussion of Independent Claim 10

Alattar does not disclose or remotely suggest using a combination of fingerprints and watermarks for reliable identification of embedded watermarks by registering both the watermark value and the fingerprint. As discussed above, the only section of Alattar dealing with a combination of watermarking and fingerprinting describes using a watermark as a calibration signal to help align the content before derivation of fingerprint data (Col. 20, lines 25-55).

Discussion of Claim 17

Figure 1 of US 6,505,160 relied on by the Examiner and incorporated into the disclosure of Alattar describes a registration process comprising sending information such as title artist name, etc., and in response receiving an identifier (Fig. 1, and Col. 4, lines 1-6). In Applicants' claim 17, there is no identification information that is sent back to the embedding process. Rather, in claim 17, information comprising the watermark value and fingerprint are received at a registration authority and verified. The subject matter of claim 17 is thus not disclosed or suggested in Alattar or US 6,505,160.

Discussion of Claim 20

As discussed above in connection with claim 17, in the registration process described in US 6,505,160, when an object already has an assigned identifier, that identifier is returned and the registration process is completed (Col. 10, lines 30-36). This is contrary to Applicants' claim 20, where finding a match is indicative of an incomplete registration.

Discussion of claim 21

Col. 10, lines 24-30 of US 6,505,160 relied on by the Examiner specifies that as part of the registration, a user is prompted to provide content identification information (e.g., title and artist name, etc.) to initiate the registration process. The subject matter of Applicants' claim 21 is

to the contrary. Claim 21 states that, in case of an incomplete registration, the applicant or content owner is notified.

Discussion of Claim 23

In the registration process described in US 6,505,160 (Col. 10, lines 30-36), a user is prompted to provide content identification information (e.g., title and artist name, etc.) to initiate the registration process. This is contrary to Applicants' claim 23, where an applicant or content owner is contacted if the registration produces at least one match.

Alattar, at column 10, lines 24-30, describes user interaction (i.e., content owner uploading the version ID to a central database) but this user interaction does not occur, as required by Applicants' claim 23, when the registration produces at least one match. In fact, the uploading of any information by the user in the cited sections of Alattar seems to be initiated by the user himself, and not in the course of registration of the content.

Discussion of Claims 24 and 25

Applicants' claims 24 and 25, which depend from claim 10 via claim 17, relate to the process of registering the content as opposed to the cited portions of Alattar relied on by the Examiner (Col. 5. lines 59-63), which describes embedding different watermark messages (i.e., information about various entities in the distribution chain, the distributor, etc.).

Discussion of Independent Claim 32

As discussed above, Alattar, in column 20, lines 20-35, teaches that detection of watermarks is used to provide alignment prior to computing the fingerprint, so that subsequently fewer fingerprints may be maintained for a content title in a fingerprint database. In contrast, with Applicants' claim 32, the generation of fingerprint is independent of the analyzing of the received content to discern the presence of embedded watermarks. With Applicants' invention as set forth in claim 32, once a fingerprint associated with the received content is generated and the received

content is analyzed to discern the presence of embedded watermarks, the received content is identified using at least one of the fingerprint and said analyzing.

US 6,505,160, at column 10, lines 29-35 relied on by the Examiner describes the registration process of the content, and is not related to receiving a content and analyzing it to discern the presence of embedded watermarks.

Thus, Alattar does not disclose or remotely suggest the subject matter of Applicants' independent claim 32.

Discussion of Claim 34

US 6,505,160 at column 10, lines 19-35 provides that as part of the registration process, a user is prompted to provide content identification information (e.g., title and artist name, etc.) to initiate the registration process. If a match in the database is found, that identifier is sent back to the user. If no match is found, then a new identifier is created in the database. This registration process is not based on detection (or absence) of watermarks in the content due the analyzing of the content, as is required by Applicants' claim 34. To the contrary, this identification seems to only rely on comparing the user entered identification information that is searched against a database of information.

Accordingly, Alattar does not disclose or remotely suggest the subject matter of Applicants' claim 34.

Discussion of Claim 35

As discussed above, the section of US 6,505,160 relied on by the Examiner pertains to the registration process (and not identification of a received content), and requires contacting the user in order to initiate this registration process. In contrast, with Applicants' claim 35, reception of unregistered content is reported in the event that there is a failure to detect watermarks, and failure to detect a match between the generated fingerprint from the receive content and a database of registered fingerprints.

Paragraph 7, lines 17-11 of US 2002/0126872 relied on by the Examiner specifies that:

content signature also may be stored or otherwise attached with the content item itself, such as in a header (or footer) or frame headers of the content item. Evidence of content tampering can be identified with an attached signature. Such identification is made through re-deriving a content signature using the same technique as was used to derive the content signature stored in the header. The newly derived signature is compared with the stored signature. If the two signatures fail to match (or otherwise coincide), the content item can be deemed altered or otherwise tampered with.

(Emphasis added). This reference does not disclose or remotely suggest any comparison of a derived fingerprint with a database of registered fingerprints, as claimed in Applicants' claim 35.

Discussion of Claim 36

The arguments set forth above with regard to independent claim 2 apply equally to Applicants' claim 36. In particular, Alattar does not disclose or remotely suggest that a detected watermark and the fingerprint are combined to uniquely identify the received content, as claimed by Applicants.

Discussion of Claim 37

The cited sections of Alattar do not describe extracting a watermark value and generating a fingerprint from the received content (see arguments set forth above with regard to Claim 2).

In addition, paragraph 11, lines 5-12 of US 2002/0126872 relied on by the Examiner specify:

The watermark data may contain a content signature and can be compared to the content signature at a later time to determine if the content is authentic. As discussed above regarding a frame header, a content signature can be compared to digital watermark data, and if the content signature and digital watermark data match (or otherwise coincide) the content is determined to be authentic. If different, however, the content is considered modified.

(emphasis added). The cited sections merely teach that the digital watermark data containing a content signature is compared to the content signature that is obtained at a later time. There are no teachings or suggestions in this cited reference to indicate that, if the fingerprint generated from the received content matches the fingerprints from the database, a first ID information associated with the stored watermark is compared with a second ID information associated with that fingerprint, as set forth in Applicants' claim 37. Claim 37 involves at least three pieces of information: watermark value, fingerprint, and Identification. In contrast, the cited section of the reference relied on by the Examiner involves at most two, and arguably only one, piece of information: the watermark data which contains the content signature.

Accordingly, Alattar does not disclose or remotely suggest the subject matter of Applicants' claim 37.

As Alattar does not disclose each and every element of the invention as claimed in claims 1, 2, 4-14, and 17-42, the rejections under 35 U.S.C. § 102(e) are believed to be improper, and withdrawal of the rejections is respectfully requested. See, *Akamai Technologies Inc., supra.*

Applicants respectfully submit that the present invention is not anticipated by and would not have been obvious to one skilled in the art in view of Alattar, taken alone or in combination with Baker or any of the other prior art of record.

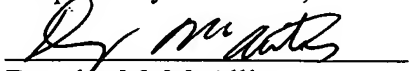
Further remarks regarding the asserted relationship between Applicants' claims and the prior art are not deemed necessary, in view of the amended claims and the foregoing discussion. Applicants' silence as to any of the Examiner's comments is not indicative of an acquiescence to the stated grounds of rejection.

Withdrawal of the rejections under 35 U.S.C. § 102(e) and 35 U.S.C. § 103(a) is therefore respectfully requested.

Conclusion

The Examiner is respectfully requested to reconsider this application, allow each of the pending claims and to pass this application on to an early issue. If there are any remaining issues that need to be addressed in order to place this application into condition for allowance, the Examiner is requested to telephone Applicants' undersigned attorney.

Respectfully submitted,



Douglas M. McAllister
Attorney for Applicant(s)
Registration No. 37,886
Lipsitz & McAllister, LLC
755 Main Street, Bldg. 8
Monroe, CT 06468
(203) 459-0200

Date: January 17, 2008
ATTORNEY DOCKET NO.: SOL-186